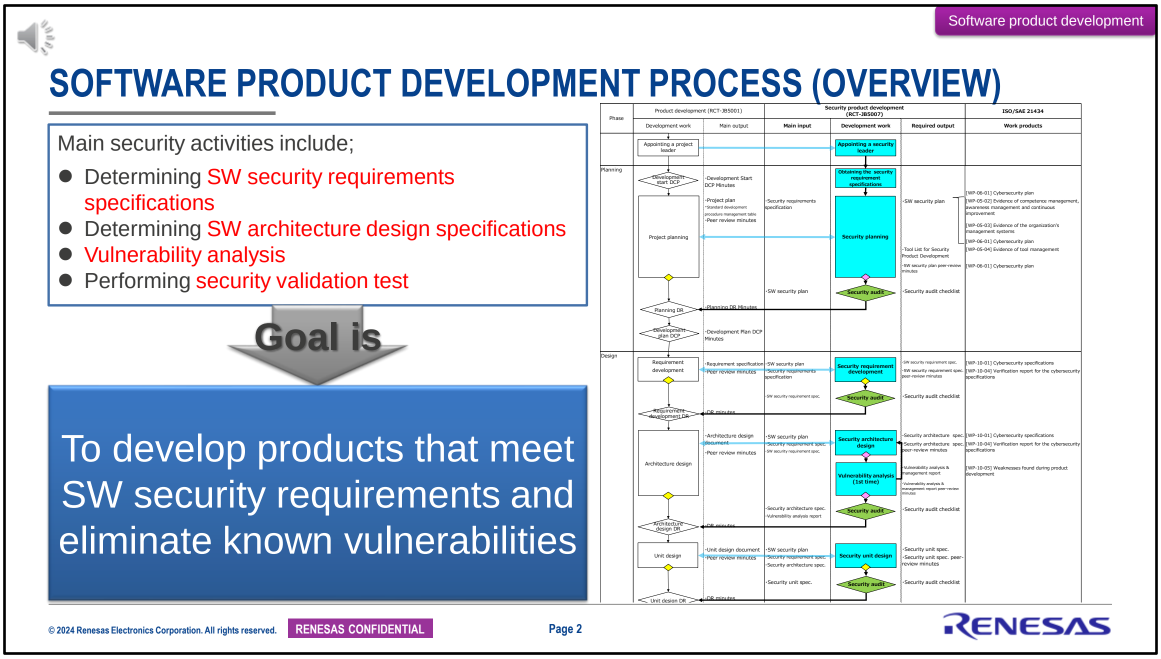
3. SOFTWARE PRODUCT DEVELOPMENT

RENESAS CONFIDENTIAL

Page 1

This video is a lecture video about the software product development process, which is part of the security product development process.



SOFTWARE PRODUCT DEVELOPMENT PROCESS (OVERVIEW)

Main security activities include;

- Determining SW security requirements specifications
- Determining SW architecture design specifications
- Vulnerability analysis
- Performing security validation test

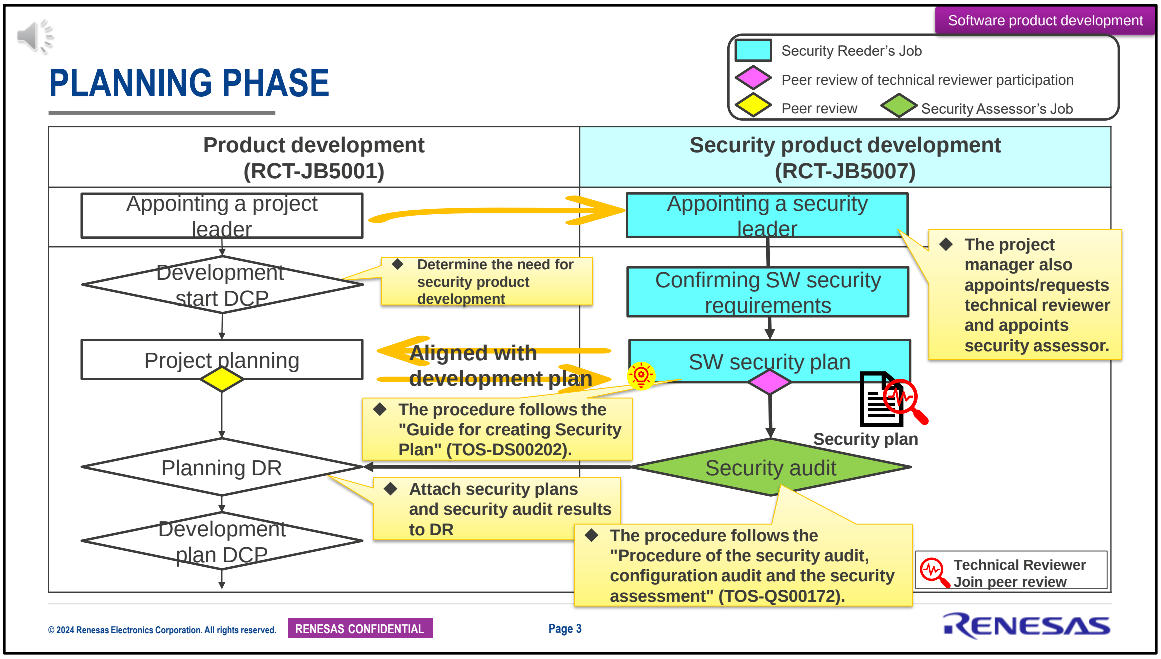
Goal is

To develop products that meet SW security requirements and eliminate known vulnerabilities

Phase	Product development (RCT-JB5001)		Security product development (RCT-JB5007)			ISO/SAE 21434
	Development work	Main output	Main input	Development work	Required output	Work products
	Appointing a project leader			Appointing a security leader		
Planning	Development start DCP	·Development Start DCP Minutes		Obtaining the security requirement specifications		
	Project planning	·Project plan ·Standard development procedure management table ·Peer review minutes	·Security requirements specification	Security planning	·SW security plan ·Tool List for Security Product Development ·SW security plan peer-review minutes	[WP-06-01] Cybersecurity plan [WP-05-02] Evidence of competence management, awareness management and continuous improvement [WP-05-03] Evidence of the organization's management systems [WP-06-01] Cybersecurity plan [WP-05-04] Evidence of tool management [WP-06-01] Cybersecurity plan
			·SW security plan	Security audit	·Security audit checklist	
	Planning DR	·Planning DR Minutes				
	Development plan DCP	·Development Plan DCP Minutes				
Design	Requirement development	·Requirement specification ·Peer review minutes	·SW security plan ·Security requirements specification	Security requirement development	·SW security requirement spec. ·SW security requirement spec. peer-review minutes	[WP-10-01] Cybersecurity specifications [WP-10-04] Verification report for the cybersecurity specifications
			·SW security requirement spec.	Security audit	·Security audit checklist	
	Requirement development DR	·DR minutes				
	Architecture design	·Architecture design document ·Peer review minutes	·SW security plan ·Security requirement spec. ·SW security requirement spec.	Security architecture design	·Security architecture spec. ·Security architecture spec. peer-review minutes	[WP-10-01] Cybersecurity specifications [WP-10-04] Verification report for the cybersecurity specifications
				Vulnerability analysis (1st time)	·Vulnerability analysis & management report ·Vulnerability analysis & management report peer-review minutes	[WP-10-05] Weaknesses found during product development
			·Security architecture spec. ·Vulnerability analysis report	Security audit	·Security audit checklist	
	Architecture design DR	·DR minutes				
	Unit design	·Unit design document ·Peer review minutes	·SW security plan ·Security requirement spec. ·Security architecture spec.	Security unit design	·Security unit spec. ·Security unit spec. peer-review minutes	
			·Security unit spec.	Security audit	·Security audit checklist	
	Unit design DR	·DR minutes				

This is an overview of the software product development process.
Just like the hardware, we have a security colorful chart on the right.
This is a diagram of the software development part.
White square indicates QM development of RCT-JB5001. The activities specified in RCT-JB5007, Security Development Process, are shown in blue and green.
In the following pages, we explain the process step by step.
Security activities carried out in software development are similar to those for hardware: determining the specifications of software security requirements, analyzing whether or not there are vulnerabilities against the determined specifications, and designing the software architecture. We conduct security validation tests on a regular basis.
The goal is to develop software products that, like hardware, meet software security requirements and are free of known vulnerabilities.

Now let's talk about the development phase.



Software product development

PLANNING PHASE

🟦 Security Reeder's Job
🟪 Peer review of technical reviewer participation
🟨 Peer review 🟩 Security Assessor's Job

Product development (RCT-JB5001)	Security product development (RCT-JB5007)
Appointing a project leader	Appointing a security leader
Development start DCP	Confirming SW security requirements
Project planning	SW security plan
Planning DR	Security audit
Development plan DCP	

- Determine the need for security product development
- The project manager also appoints/requests technical reviewer and appoints security assessor.
- The procedure follows the "Guide for creating Security Plan" (TOS-DS00202).
- Attach security plans and security audit results to DR
- The procedure follows the "Procedure of the security audit, configuration audit and the security assessment" (TOS-QS00172).

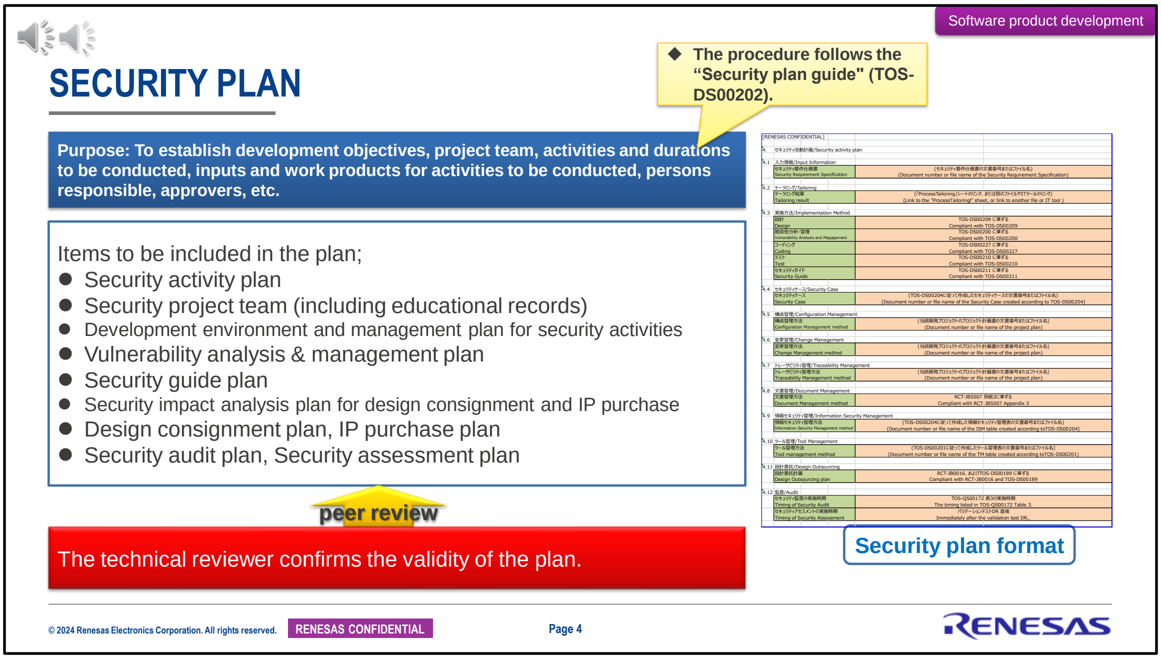
Technical Reviewer Join peer review

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 3

RENESAS

This is the planning phase.
In the software development planning phase, we first appoint a project leader for RCT-JB5001. Along with the appointment of a project leader, if a security-compatible product is to be developed, a security leader is also appointed.
Once a security leader has been determined, that project manager requests the appointment of technical reviewers necessary for security development and security assessors to conduct audits and assessments.
If security product development is determined to be necessary during development start deliberations, a project plan is created in accordance with RCT-JB5001. At the stage of creating a project plan, for security, we formulate a security plan, which was explained earlier regarding hardware. For software, we have already prepared and released a security plan template, so please create your security plan in accordance with that template. Once the security plan has been created, it undergoes a peer review that includes technical reviewers, passes peer review, and undergoes a security audit by the quality department. Security audits are conducted at the end of the planning

phase specified in RCT-JB5001. The results of the security audit are included in the Plan D R as one of its deliberation items.



Software product development

SECURITY PLAN

◆ The procedure follows the "Security plan guide" (TOS-DS00202).

Purpose: To establish development objectives, project team, activities and durations to be conducted, inputs and work products for activities to be conducted, persons responsible, approvers, etc.

Items to be included in the plan;

- Security activity plan
- Security project team (including educational records)
- Development environment and management plan for security activities
- Vulnerability analysis & management plan
- Security guide plan
- Security impact analysis plan for design consignment and IP purchase
- Design consignment plan, IP purchase plan
- Security audit plan, Security assessment plan

peer review

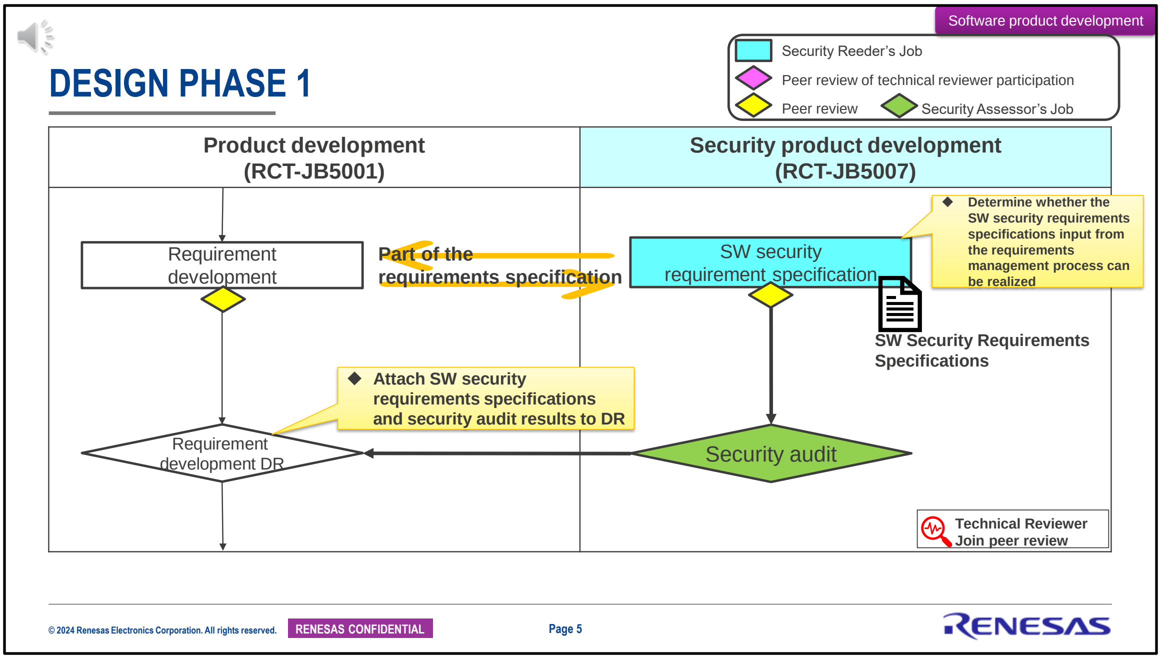
The technical reviewer confirms the validity of the plan.

[RENESAS CONFIDENTIAL]

4.	セキュリティ活動計画/Security activity plan	
4.1	入力情報/Input Information	
	セキュリティ要件仕様書 Security Requirement Specification	(セキュリティ要件仕様書の文書番号またはファイル名) (Document number or file name of the Security Requirement Specification)
4.2	テーラリング/Tailoring	
	テーラリング結果 Tailoring result	(「ProcessTailoring」シートのリンク、または別のファイルやITツールのリンク) (Link to the "ProcessTailoringl" sheet, or link to another file or IT tool)
4.3	実施方法/Implementation Method	
	設計 Design	TOS-DS00209 に準ずる Compliant with TOS-DS00209
	脆弱性分析・管理 Vulnerability Analysis and Magagement	TOS-DS00200 に準ずる Compliant with TOS-DS00200
	コーディング Coding	TOS-DS00227 に準ずる Compliant with TOS-DS00227
	テスト Test	TOS-DS00210 に準ずる Compliant with TOS-DS00210
	セキュリティガイド Security Guide	TOS-DS00211 に準ずる Compliant with TOS-DS00211
4.4	セキュリティケース/Security Case	
	セキュリティケース Security Case	(TOS-DS00204に従って作成したセキュリティケースの文書番号またはファイル名) (Document number or file name of the Security Case created according to TOS-DS00204)
4.5	構成管理/Configuration Management	
	構成管理方法 Configuration Management method	(当該開発プロジェクトのプロジェクト計画書の文書番号またはファイル名) (Document number or file name of the project plan)
4.6	変更管理/Change Management	
	変更管理方法 Change Management method	(当該開発プロジェクトのプロジェクト計画書の文書番号またはファイル名) (Document number or file name of the project plan)
4.7	トレーサビリティ管理/Traceability Management	
	トレーサビリティ管理方法 Traceability Management method	(当該開発プロジェクトのプロジェクト計画書の文書番号またはファイル名) (Document number or file name of the project plan)
4.8	文書管理/Document Management	
	文書管理方法 Document Management method	RCT-JB5007 別紙3に準ずる Compliant with RCT-JB5007 Appendix 3
4.9	情報セキュリティ管理/Information Security Management	
	情報セキュリティ管理方法 Information Security Management method	(TOS-DS00204に従って作成した情報セキュリティ管理表の文書番号またはファイル名) (Document number or file name of the ISM table created according toTOS-DS00204)
4.10	ツール管理/Tool Management	
	ツール管理方法 Tool management method	(TOS-DS00201に従って作成したツール管理表の文書番号またはファイル名) (Document number or file name of the TM table created according toTOS-DS00201)
4.11	設計委託/Design Outsourcing	
	設計委託計画 Design Outsourcing plan	RCT-JB0016、およびTOS-DS00189 に準ずる Compliant with RCT-JB0016 and TOS-DS00189
4.12	監査/Audit	
	セキュリティ監査の実施時期 Timing of Security Audit	TOS-QS00172 表3の実施時期 The timing listed in TOS-QS00172 Table 3.
	セキュリティアセスメントの実施時期 Timing of Security Assessment	バリデーションテストDR 直後 Immediately after the validation test DR,.

Security plan format

This is the implementation content of the security plan.
Items to include in the security plan include:
This is shown in the black circle here.
This one,
The security plan form that has already been released has columns for each item. Please use this form to fill in the details of your plan in accordance with the actual development details.
Once the project has created a security plan, it undergoes a peer review, including technical reviewers.
During the peer review, the technical reviewer confirms the sufficiency and validity of the plan with respect to the items and contents included in the plan, and points out any deficiencies.



Software product development

DESIGN PHASE 1

🟦 Security Reeder's Job
◆ Peer review of technical reviewer participation
◆ Peer review ◆ Security Assessor's Job

Product development (RCT-JB5001)	Security product development (RCT-JB5007)

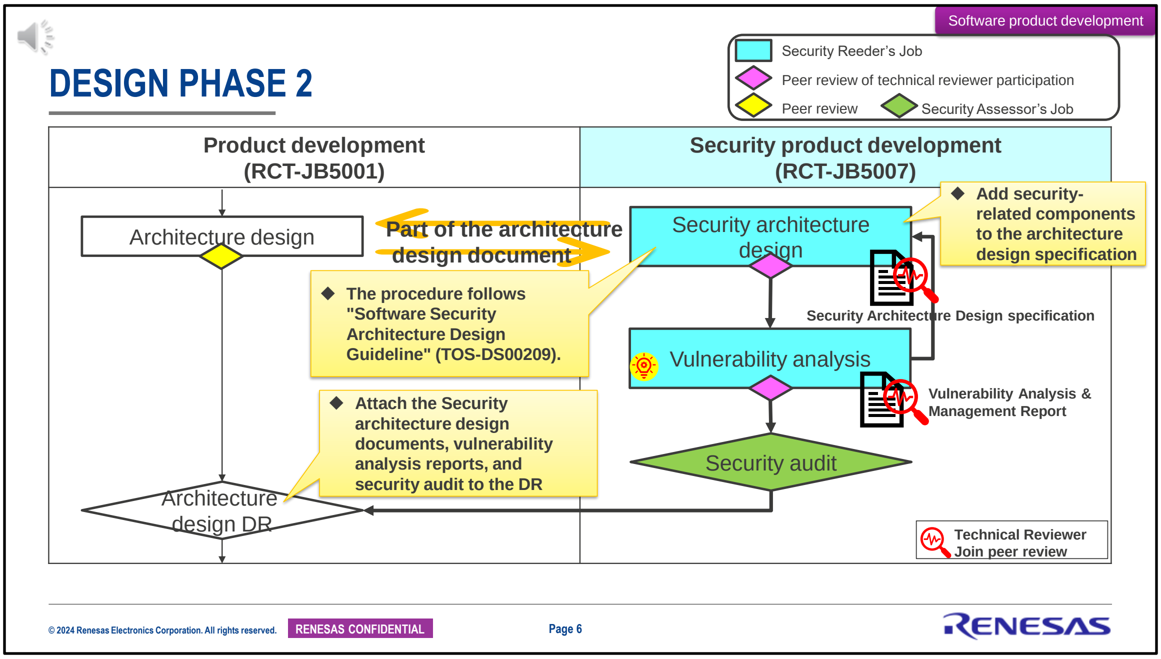
Requirement development
Part of the requirements specification
SW security requirement specification
SW Security Requirements Specifications
Requirement development DR
Security audit
Technical Reviewer Join peer review

- Determine whether the SW security requirements specifications input from the requirements management process can be realized

- Attach SW security requirements specifications and security audit results to DR

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 5 RENESAS

Next, we move on to an explanation of the design phase.
In software development, after the planning phase, design activities for requirements development are carried out.
Along with this requirements development, software security requirements are developed for security compatible products. Here, the requirements for software development are set by determining whether or not the security requirements for the software input from the requirements management process can be realized in software development.
Once software security requirements are determined, a security audit is performed on these design activities. The results of the security audit are passed on to the requirements development department.



Software product development

DESIGN PHASE 2

🟦 Security Reeder's Job
◆ Peer review of technical reviewer participation
◆ Peer review ◆ Security Assessor's Job

Product development (RCT-JB5001)	Security product development (RCT-JB5007)

Architecture design

Part of the architecture design document

Security architecture design

- Add security-related components to the architecture design specification

- The procedure follows "Software Security Architecture Design Guideline" (TOS-DS00209).

Security Architecture Design specification

Vulnerability analysis

Vulnerability Analysis & Management Report

- Attach the Security architecture design documents, vulnerability analysis reports, and security audit to the DR

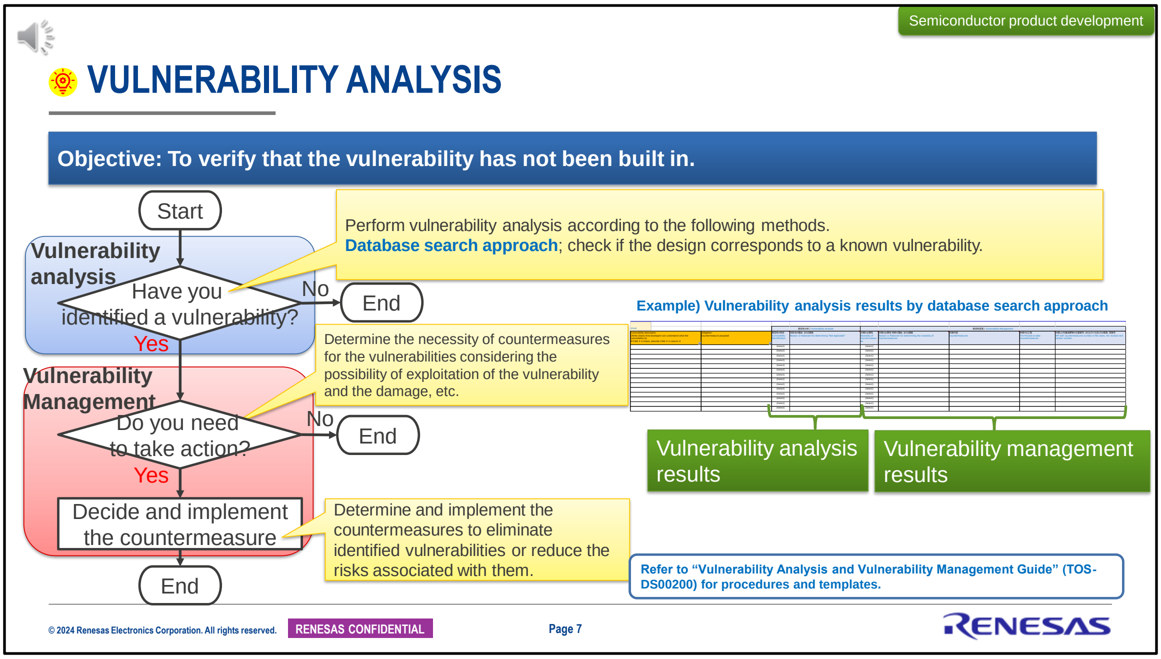
Security audit

Architecture design DR

Technical Reviewer Join peer review

RENESAS CONFIDENTIAL Page 6 RENESAS

Once the requirements development activities are complete, the next step is architecture design activities.
When implementing RCT-JB5001 architecture design activities, security-enabled product development involves implementing architecture design specific to software security requirements.
Once the architecture has been designed to meet software security requirements, the next step is vulnerability analysis.
We have already prepared and released a vulnerability analysis management report template, so please create your vulnerability analysis management report in accordance with that template.
Once the vulnerability analysis management report is created, it is peer reviewed, including by technical reviewers, and after that peer review, the quality department conducts a security audit and then a design review.



Semiconductor product development

VULNERABILITY ANALYSIS

Objective: To verify that the vulnerability has not been built in.

Start
Vulnerability analysis
Have you identified a vulnerability?
No
End
Yes
Vulnerability Management
Do you need to take action?
No
End
Yes
Decide and implement the countermeasure
End

Perform vulnerability analysis according to the following methods.
Database search approach; check if the design corresponds to a known vulnerability.

Determine the necessity of countermeasures for the vulnerabilities considering the possibility of exploitation of the vulnerability and the damage, etc.

Determine and implement the countermeasures to eliminate identified vulnerabilities or reduce the risks associated with them.

Example) Vulnerability analysis results by database search approach

Vulnerability analysis results
Vulnerability management results

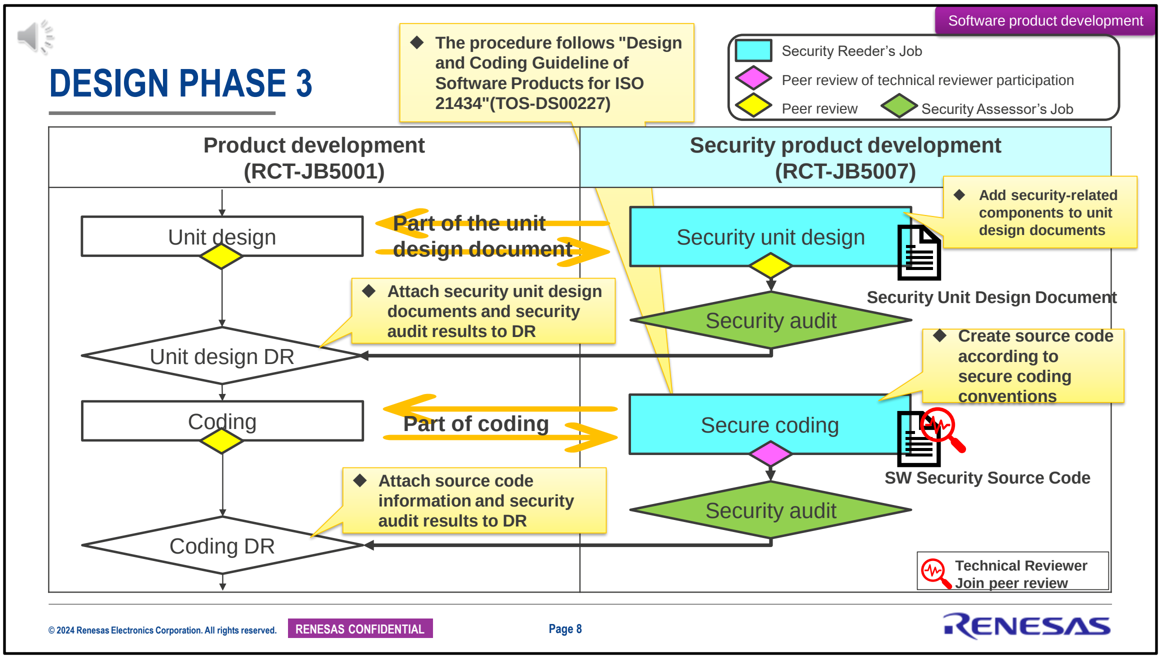
Refer to "Vulnerability Analysis and Vulnerability Management Guide" (TOS-DS00200) for procedures and templates.

RENESAS CONFIDENTIAL Page 7 RENESAS

In this page, we explain the vulnerability analysis.
Vulnerability analysis is performed at this architecture design stage.
Vulnerability analysis is equivalent to vulnerability analysis, which was explained earlier in hardware design, but the only difference is whether it deals with hardware requirements or software requirements, and whether there is a vulnerability or not. The search for the vulnerability and its treatment are carried out in the same way as for the hardware.

If vulnerability analysis is performed and vulnerabilities are identified, vulnerability management is required.
Decide whether countermeasures are required and record the results of implementing the countermeasures.
Vulnerability analysis and vulnerability management are thus performed as a set during the development process.
As an example, we have posted the format of a vulnerability analysis management report using a database search approach.
This report also allows you to record both vulnerability analysis results and vulnerability management results.

Vulnerability management is covered in part 4, the management process.



Software product development

DESIGN PHASE 3

- The procedure follows "Design and Coding Guideline of Software Products for ISO 21434"(TOS-DS00227)

▭ Security Reeder’s Job
◆ Peer review of technical reviewer participation
◆ Peer review ◆ Security Assessor’s Job

Product development (RCT-JB5001)

Security product development (RCT-JB5007)

Unit design

Part of the unit design document

Security unit design

- Add security-related components to unit design documents

Security Unit Design Document

- Attach security unit design documents and security audit results to DR

Security audit

Unit design DR

- Create source code according to secure coding conventions

Coding

Part of coding

Secure coding

SW Security Source Code

- Attach source code information and security audit results to DR

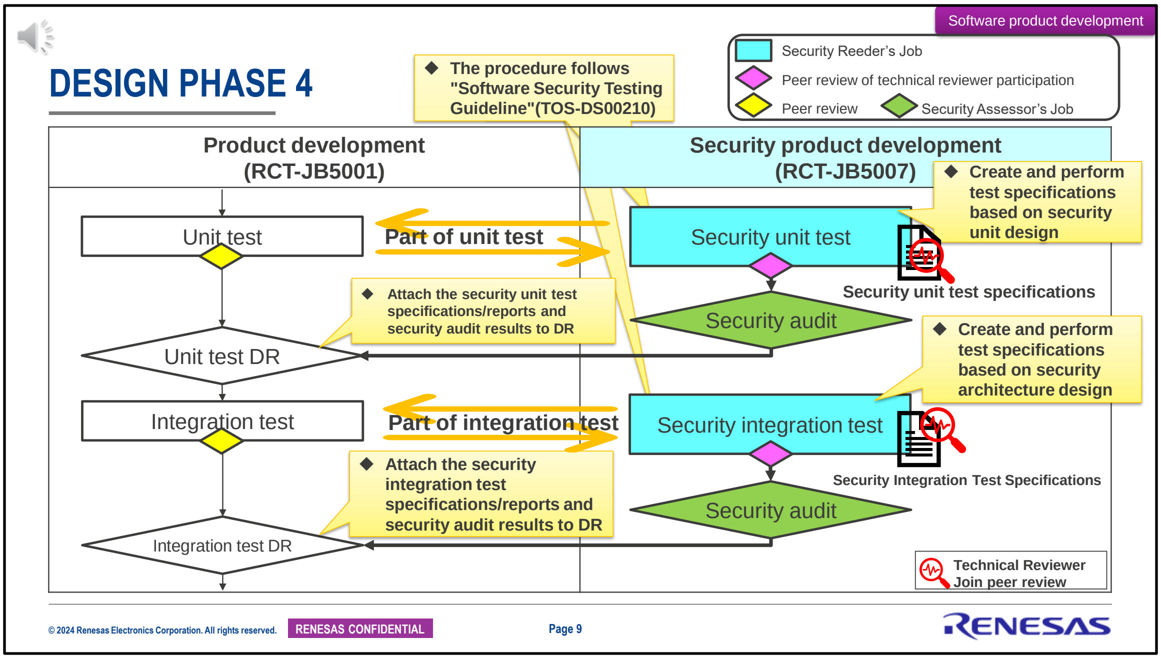
Security audit

Coding DR

Technical Reviewer
Join peer review

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 8 RENESAS

Once the architectural design activities are completed, the next step is unit design and coding activities to create the source code.
Regarding unit design and coding activities, at each stage of design activities, we focus on the software security requirements set in requirements development activities, perform security unit design, and perform secure coding.
Upon completion of each design activity, a peer review and security audit are conducted. Current regulations do not stipulate the participation of technical reviewers in peer reviews of unit designs.
However, if you need to check the sufficiency and validity of the technical content, please invite technical reviewers to participate. On the other hand, in secure coding, a peer review with a technical reviewer present is specified, so during this peer review, the created code is reviewed to see if it is appropriate from a security technology perspective.



Software product development

DESIGN PHASE 4

- The procedure follows "Software Security Testing Guideline"(TOS-DS00210)

🟦 Security Reeder's Job
◆ Peer review of technical reviewer participation
◆ Peer review
◆ Security Assessor's Job

Product development (RCT-JB5001)

Security product development (RCT-JB5007)

Unit test

Part of unit test

Security unit test

- Create and perform test specifications based on security unit design

Security unit test specifications

Security audit

- Attach the security unit test specifications/reports and security audit results to DR

Unit test DR

Integration test

Part of integration test

Security integration test

- Create and perform test specifications based on security architecture design

Security Integration Test Specifications

Security audit

- Attach the security integration test specifications/reports and security audit results to DR

Integration test DR

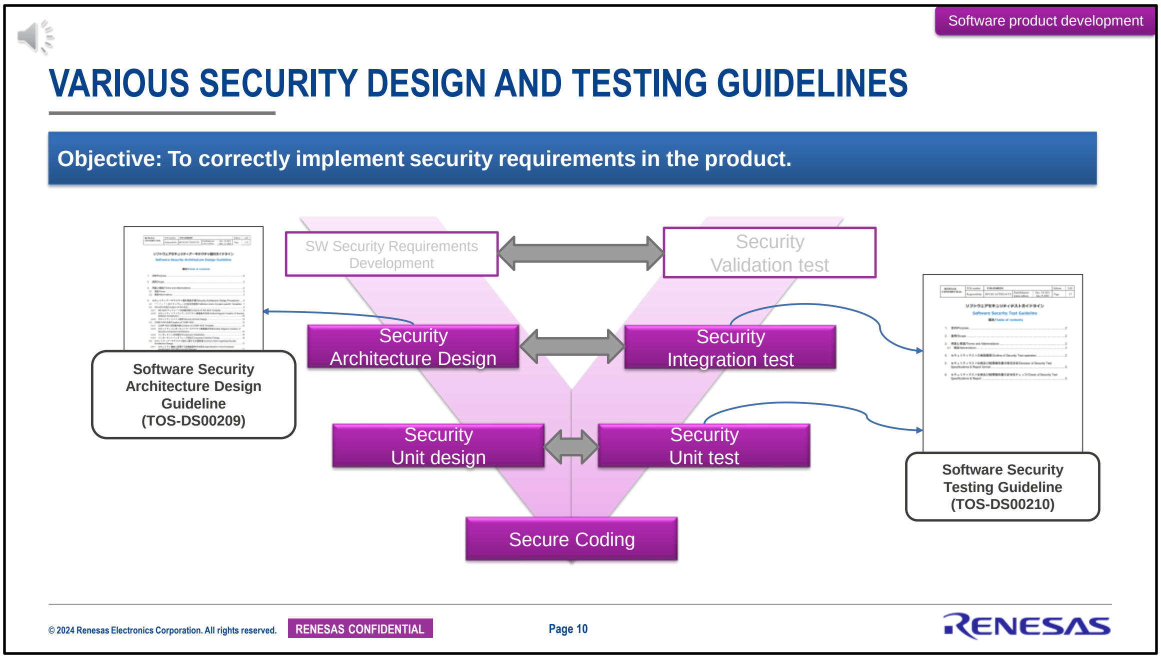
Technical Reviewer Join peer review

RENESAS CONFIDENTIAL

Page 9

RENESAS

Next, now that the software is complete, we will move on to verification activities.
Unit testing and integration testing: Similar to design activities, we conduct tests on each unit focusing on software security requirements, and integration tests that integrate one or more units.
The flow of security development here is also to create test specifications, conduct tests, undergo a security audit, and then conduct a design review integrated with QM development.
In right side, security unit tests and security integration tests, there is a pink sign stating that it is mandatory to have a technical reviewer participate in peer reviews. Technical reviewers are required to attend peer reviews of test specifications and test items, such as unit test specifications and integration test specifications, as with hardware. It does not stipulate that technical reviewers are required to attend peer reviews of test results conducted in accordance with test specifications. This is implemented using the same concept as with hardware.



Software product development

VARIOUS SECURITY DESIGN AND TESTING GUIDELINES

Objective: To correctly implement security requirements in the product.

SW Security Requirements Development

Security Validation test

Security Architecture Design

Security Integration test

Security Unit design

Security Unit test

Secure Coding

Software Security Architecture Design Guideline (TOS-DS00209)

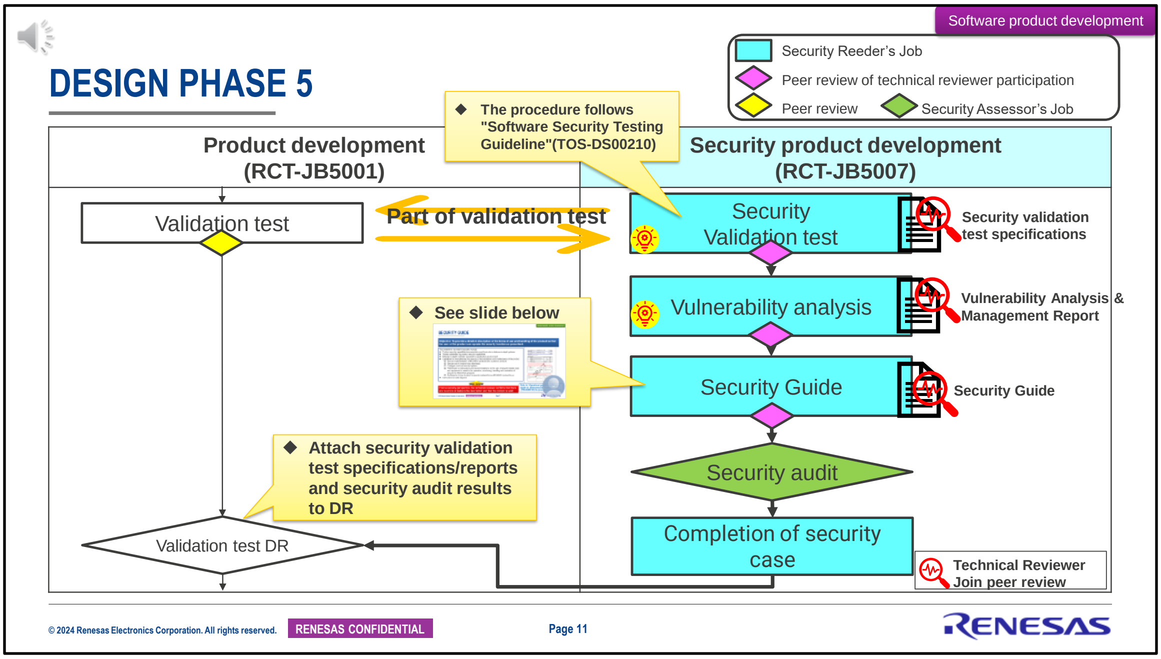
Software Security Testing Guideline (TOS-DS00210)

RENESAS CONFIDENTIAL

Page 10

RENESAS

I'll provide an explanation here to help you with your design.
I'm sure anyone involved in software development has seen this before. This shows the model for the development of that V character. Among them, security architecture design, security unit testing, and security integration testing. In addition to RCT rules, we have created guidelines for each of these three design activities. When carrying out each design activity, please read these guidelines, understand the contents, and carry out design activities in accordance with these guidelines.



Software product development

DESIGN PHASE 5

- ■ Security Reeder's Job
- ◆ Peer review of technical reviewer participation
- ◆ Peer review
- ◆ Security Assessor's Job

◆ The procedure follows "Software Security Testing Guideline"(TOS-DS00210)

Product development (RCT-JB5001)

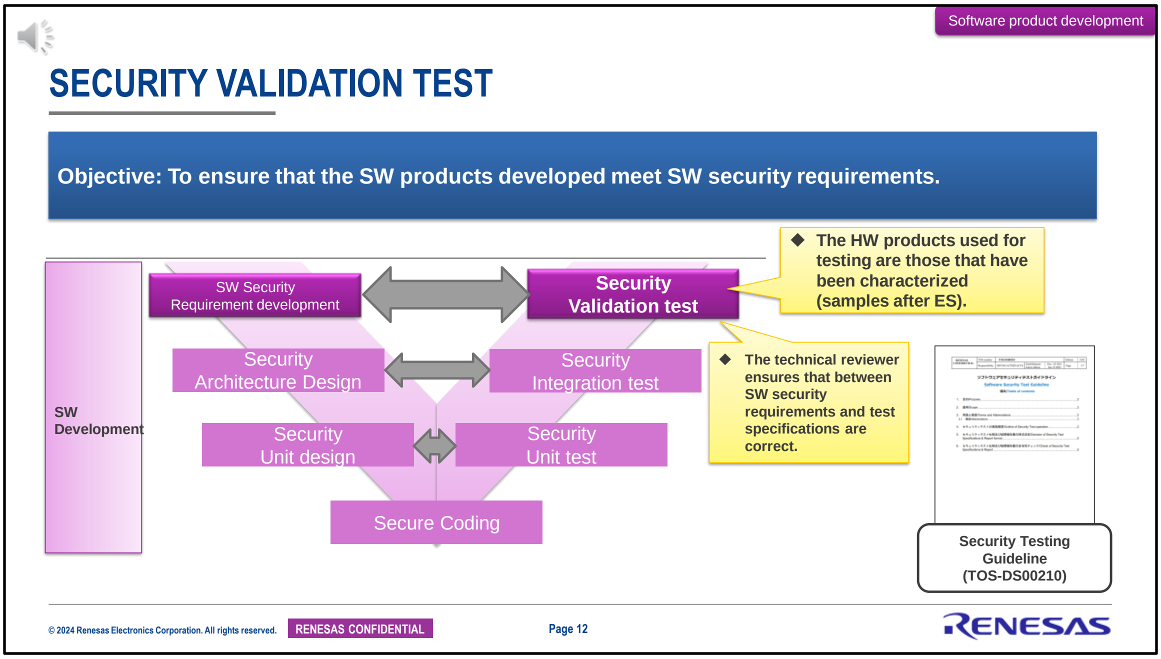
Security product development (RCT-JB5007)

◆ See slide below

◆ Attach security validation test specifications/reports and security audit results to DR

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 11 RENESAS

Let's go back to the development flow.
We will explain the validation test that is performed at the end of the design phase. When conducting validation tests, security product developers also perform validation tests in the same way.
Once the validation test is complete, we then conduct a vulnerability analysis. After that, we create a security guide for the software development product, conduct an audit, and move on to validation testing. The next page describes security validation testing.



Software product development

SECURITY VALIDATION TEST

Objective: To ensure that the SW products developed meet SW security requirements.

SW Development

SW Security Requirement development

Security Validation test

Security Architecture Design

Security Integration test

Security Unit design

Security Unit test

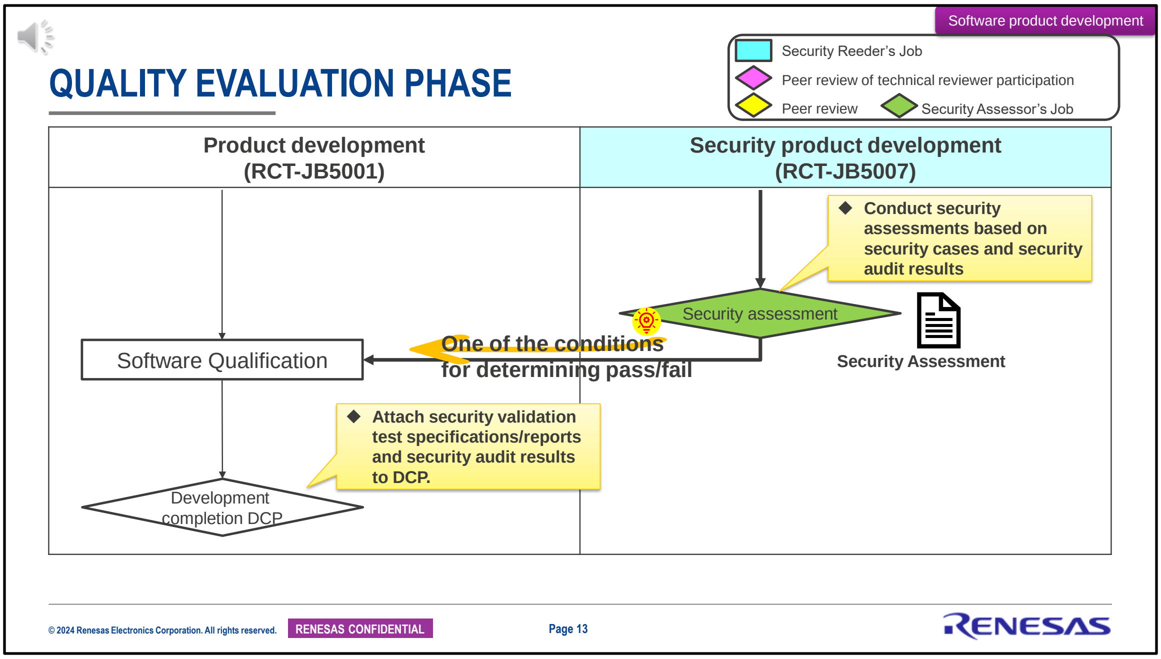
Secure Coding

- ◆ **The HW products used for testing are those that have been characterized (samples after ES).**
- ◆ **The technical reviewer ensures that between SW security requirements and test specifications are correct.**

Security Testing Guideline (TOS-DS00210)

© 2024 Renesas Electronics Corporation. All rights reserved. RENESAS CONFIDENTIAL Page 12 RENESAS

The validation test for RCT-JB5001 is positioned as a verification of the validity of the software requirements set during requirements development. This position remains the same in security product development.
Regarding the hardware used in validation tests, we specify samples for which characteristic evaluation of hardware product development has been completed, and samples from E S and later. Please conduct validation tests for software security requirements using a combination of hardware and software that meets the conditions. We also provide guidelines for security validation tests, so please use them as an aid to your design activities.



Software product development

QUALITY EVALUATION PHASE

🟦 Security Reeder’s Job
◆ Peer review of technical reviewer participation
◆ Peer review
◆ Security Assessor’s Job

Product development (RCT-JB5001)	Security product development (RCT-JB5007)

Software Qualification

Development completion DCP

- Attach security validation test specifications/reports and security audit results to DCP.

Security assessment

- Conduct security assessments based on security cases and security audit results

Security Assessment

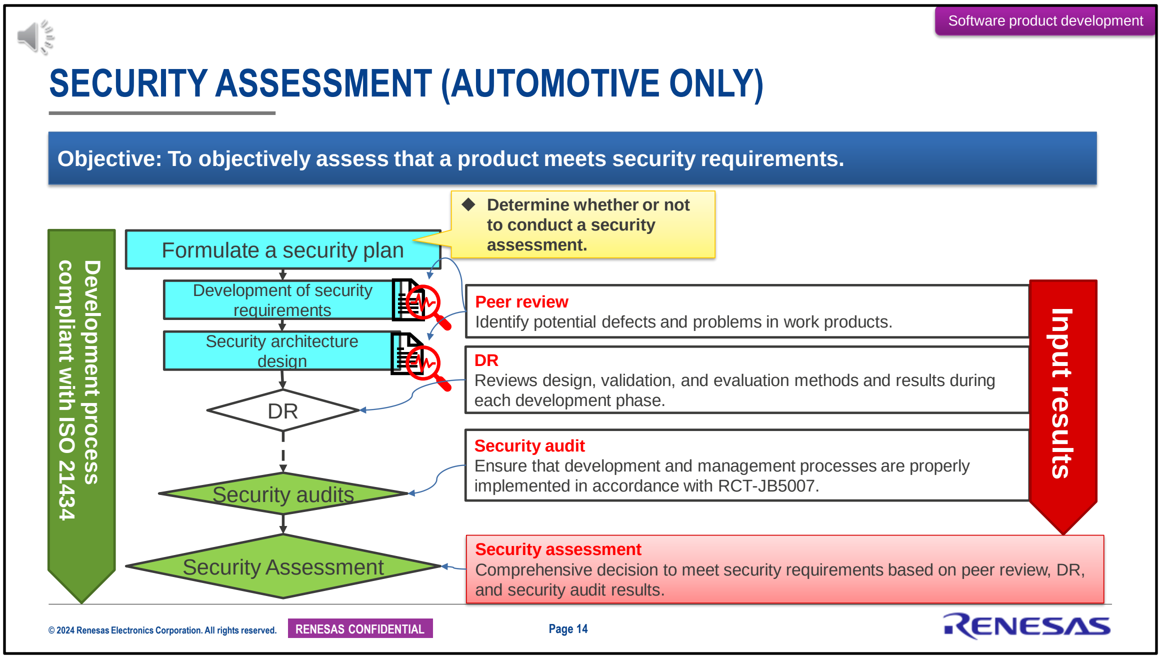
One of the conditions for determining pass/fail

RENESAS CONFIDENTIAL

Page 13

RENESAS

This is the final stage of the development phase. Describe the quality evaluation phase.
Once the validation test D R is completed, we move on to the quality evaluation phase. There are no specific regulations regarding design activities here.
The quality department conducts security assessments, inputs the security assessment results into software qualification, and makes the final software qualification pass/fail judgment. The security assessment results is one condition of the software qualification pass/fail judgment.
Regarding security assessment, software and hardware have similar ideas and concepts. In particular, just because it is software, it does not mean that it is an assessment that uses assessment items other than hardware.



Software product development

SECURITY ASSESSMENT (AUTOMOTIVE ONLY)

Objective: To objectively assess that a product meets security requirements.

Development process compliant with ISO 21434

Formulate a security plan

- **Determine whether or not to conduct a security assessment.**

Development of security requirements

Security architecture design

DR

Security audits

Security Assessment

Input results

Peer review
Identify potential defects and problems in work products.

DR
Reviews design, validation, and evaluation methods and results during each development phase.

Security audit
Ensure that development and management processes are properly implemented in accordance with RCT-JB5007.

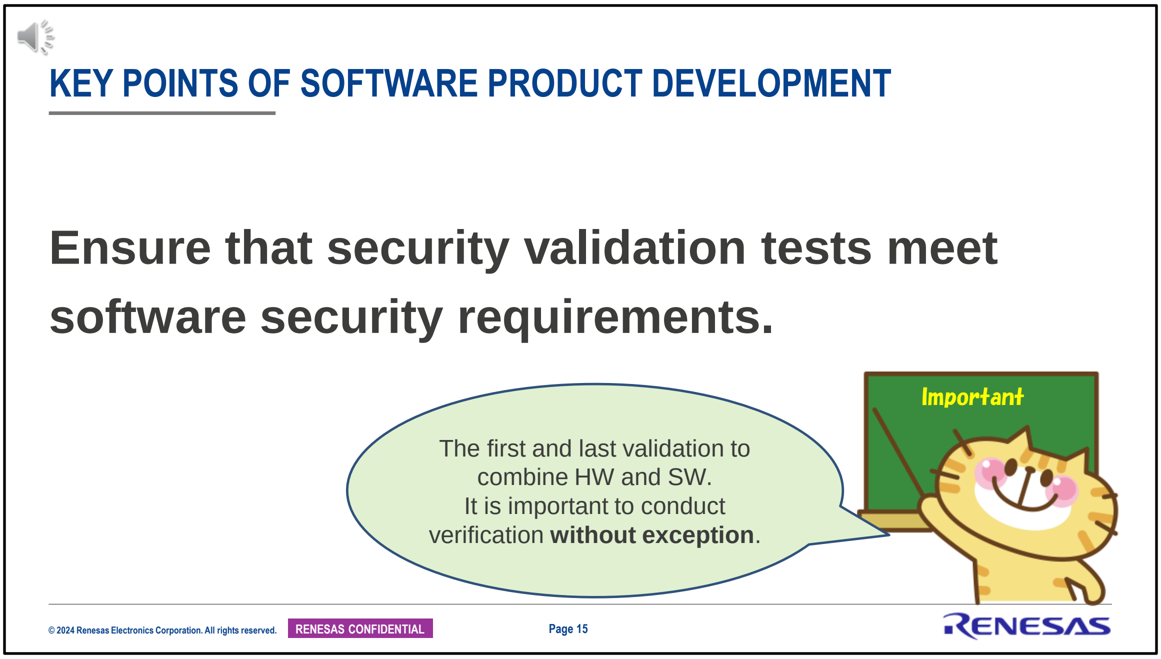
Security assessment
Comprehensive decision to meet security requirements based on peer review, DR, and security audit results.

RENESAS CONFIDENTIAL

RENESAS

This is similar to the assessment described for semiconductor product development.

In a security assessment, a third party objectively evaluates whether a product meets security requirements.
This third party could be a security assessor from the quality department who is independent from the product development team.
We integrate the results of peer reviews, D R, and security audits conducted during product development to determine whether security requirements have been achieved and pass or fail the security assessment.
Security assessments check the results of security activities based on the security cases explained on the previous page.
Security assessment procedures and formats are defined in Procedure of the Security Audit and the security Assessment, TOS-QS00172.
This security assessment report, together with the security guide and security case, are submitted to the customer based on customer agreement. Security assessors also create assessment reports for customer submission.



KEY POINTS OF SOFTWARE PRODUCT DEVELOPMENT

Ensure that security validation tests meet software security requirements.

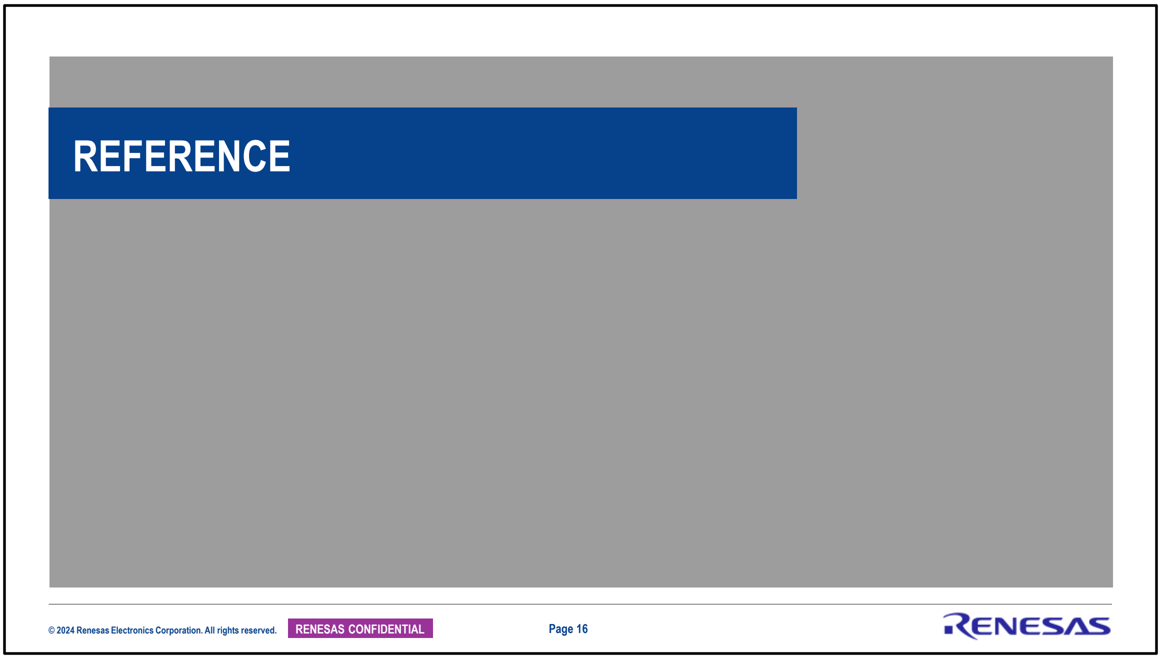
The first and last validation to combine HW and SW.
It is important to conduct verification **without exception**.

RENESAS CONFIDENTIAL

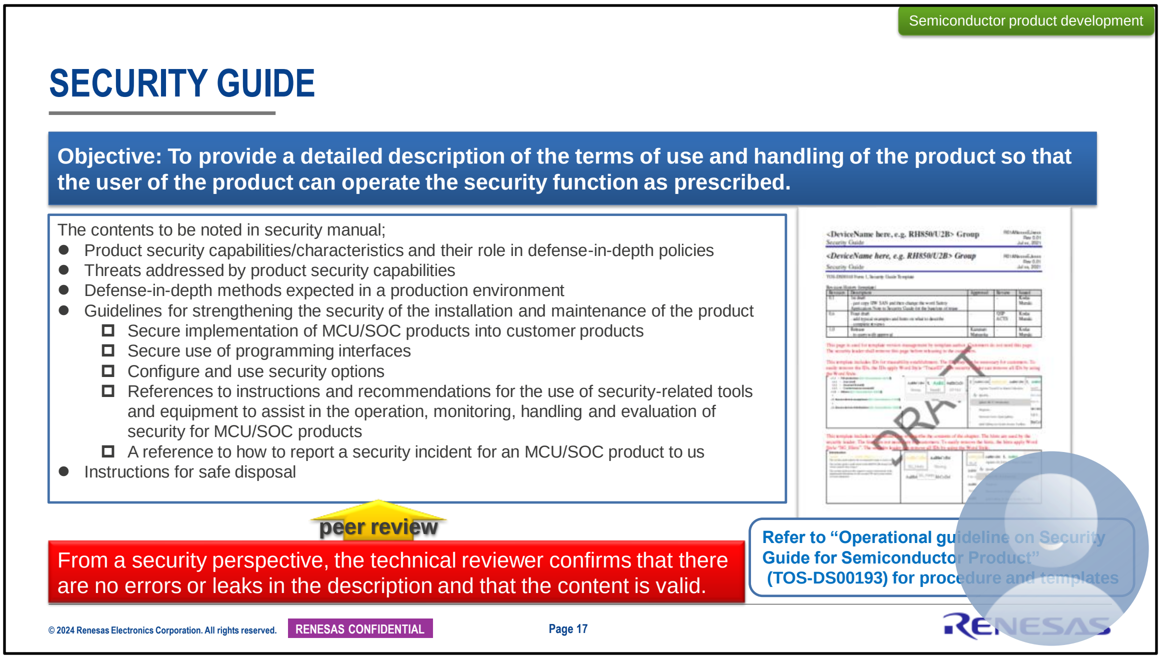
RENESAS

This concludes the explanation of the software product development process.
The key point in software product development is to achieve software security requirements at the final stage of the development process.
The key point is that confirmation through security validation testing is an important activity in security product development.

This concludes our explanation of the software product development process. Thank you for watching.



REFERENCE



SECURITY GUIDE

Objective: To provide a detailed description of the terms of use and handling of the product so that the user of the product can operate the security function as prescribed.

The contents to be noted in security manual;

- Product security capabilities/characteristics and their role in defense-in-depth policies
- Threats addressed by product security capabilities
- Defense-in-depth methods expected in a production environment
- Guidelines for strengthening the security of the installation and maintenance of the product
  - □ Secure implementation of MCU/SOC products into customer products
  - □ Secure use of programming interfaces
  - □ Configure and use security options
  - □ References to instructions and recommendations for the use of security-related tools and equipment to assist in the operation, monitoring, handling and evaluation of security for MCU/SOC products
  - □ A reference to how to report a security incident for an MCU/SOC product to us
- Instructions for safe disposal

peer review

From a security perspective, the technical reviewer confirms that there are no errors or leaks in the description and that the content is valid.

Refer to "Operational guideline on Security Guide for Semiconductor Product" (TOS-DS00193) for procedure and templates

Security guide.
The purpose of creating a security guide is to thoroughly describe the terms of use and handling of the product so that the user of the product can operate the security functions as intended.
The contents of the security guide are as follows.
It is also necessary to implement in the security guide all security guide requirements extracted during the creation of security requirements in the requirements management process, and all the requirements for components external to the product that were derived as a result of T V A conducted during semiconductor product development.
A peer review is conducted on the created security guide with the participation of technical reviewers.
From a security perspective, technical reviewers check that there are no errors or omissions in the descriptions and that the contents are valid.
For the creation procedure and format, please refer to the Operational guideline on Security Guide for Semiconductor Product, TOS-DS00193.